INPI

NATIONAL INSTITUTE
OF INDUSTRIAL
PROPERTY

PATENT

CERTIFICATE OF UTILITY - CERTIFICATE OF ADDITION

OFFICIAL COPY

The Director General of the National Institute of Industrial Property certifies that the document appended hereto is a certified true copy of an application for a certificate of patent rights filed with this office.

Issued in Paris, on: October 28, 2011

on behalf of the Director General
National Institute of Industrial Property
Head of Patent Division

[signature]

Martine PLANCHE

NATIONAL INSTITUTE OF INDUSTRIAL PROPERTY
NATIONAL PUBLIC CORPORATION

REGISTERED OFFICE
26 bis, rue de Saint-Petersbourg
75800 PARIS Cedex 08
Telephone: 33 (0)1 53 04 53 04
Fax: 33 (0)1 53 04 45 23
www.inpi-fr

FORMED UNDER LAW NO. 51-444 OF 19 APRIL 1951

INPI

PATENT
CERTIFICATE OF UTILITY

26 bis, rue de Saint-Pétersbourg
75800 Paris Cedex 08
Telephone: 01.53.05.53.04 Fax: 01 53 04 52 65

Code of Intellectual Property Rights – Book VI

APPLICATION FOR ISSUE OF CERTIFICATE

DATE OF SUBMISSION OF DOCUMENTS: NATIONAL REGISTRATION NUMBER: REGISTRATION DEPARTMENT: REGISTRATION DATE:	Gérard POULIN BREVALEX 3, rue du Docteur Lancereaux 75008 PARIS France

Your references for this file: SP 24283 HM 03-024

1 TYPE OF APPLICATION

Patent application

2 TITLE OF INVENTION

METHOD FOR MATCHING A NUMBER N OF RECEPTION TERMINALS WITH A NUMBER M OF CONDITIONAL ACCESS CONTROL CARDS

3 STATEMENT OF PRIORITY OR REQUEST TO BENEFIT FROM FILING DATE OF A PRIOR FRENCH APPLICATION

Country or organisation	Date	No.

4-1 APPLICANT

Name	VIACCESS
Street	Les Collines de l'Arche Tour Opéra C
Postcode and Town/City	92057 PARIS LA DEFENSE CEDEX
Country	France
Nationality	France
Legal form	Public limited company

5A AGENT

Name	POULIN
First name	Gérard
Quality	CPI: 99 0200, no proxy
Agency or Company	BREVALEX
Street	3 rue du Docteur Lancereaux
Postcode and Town/City	75008 PARIS
Telephone no.	01 53 83 94 00
Fax no.	01 45 63 83 33
Email	brevets.patents@brevalex.com

6 DOCUMENTS AND FILES ATTACHED	Electronic file	Pages	Details
Text of the patent	textebrevet.pdf	41	D 28, C 12, AB 1
Drawings	dessins.pdf	3	page 3, figures 7, Abstract: page 3, Fig. 7
Designation of inventors			

7 PAYMENT METHOD				
Payment method	Debit from current account			
Client account number	714			
8 SEARCH REPORT				
Immediate issue				
9 FEES ENCLOSED	CURRENCY	Rate	Quantity	Amount to pay
062 Registration	EURO	0.00	1.00	0.00
063 Search report	EURO	320.00	1.00	320.00
068 Claim from the 11th	EURO	15.00	29.00	435.00
Total due	EURO			755.00

Law n° 78-17 of 6 January 1978 on computerised data, files and personal rights applies to the answers given in this form.
It guarantees the applicant's right to access and correct the information held by the INPI office.

Signed by
Signatory: FR, BREVALEX, G. Poulin
Certificate issuer: DE, D-Trust GmbH, D-Trust for EPO 2.0
Position
Authorised agent (Agent 1)

F R E N C H R E P U B L I C

INPI

PATENT

CERTIFICATE OF UTILITY

Electronic reception of a submission

It is hereby certified that a patent (or certificate of utility) application has been received via the INPI secure electronic registration system. Following receipt, a registration number and received date have been automatically attributed.

Patent application: X
CU application:

DATE RECEIVED	20 February 2004	
REGISTRATION TYPE	INPI (PARIS) - Electronic registration	**Online registration: X** **CD Registration:**
NATIONAL REGISTRATION No. ASSIGNED BY INPI	0450324	
Your references for this file	SP 24283 HM 03-024	

APPLICANT

Name or company name	VIACCESS
Number of applicants	1
Country	FR

TITLE OF INVENTION

METHOD FOR MATCHING A NUMBER N OF RECEPTION TERMINALS WITH A NUMBER M OF CONDITIONAL ACCESS CONTROL CARDS

DOCUMENTS SENT

package-data.xml	Requetefr.PDF	fee-sheet.xml
Design.PDF	Validlog.PDF	textebrevet.pdf
FR-office-specific-info.xml	application-body.xml	request.xml
dessins.pdf	indication-bio-deposit.xml	

SUBMITTED BY

Submitted by:	G. Poulin
Date and time of electronic reception:	20 February 2004 16:10:00
Official marking of registration	20:0A:BC:1D:2C:FF:26:A3:4F:14:32:80:11:3D:CF:17:8F:5F:BB:F3

/ INPI PARIS, Filing Department /

NATIONAL INSTITUTE OF INDUSTRIAL PROPERTY

REGISTERED OFFICE
26 bis, rue de Saint-Petersbourg
75800 PARIS Cedex 08
Telephone: 33 (0)1 53 04 53 04
Fax: 33 (0)1 53 04 45 23
www.inpi-fr

NATIONAL PUBLIC CORPORATION FORMED UNDER LAW NO. 51-444 OF 19 APRIL 1951

INPI

PATENT
CERTIFICATE OF UTILITY

Designation of inventor

Your references for this file	SP 24283 03-024
NATIONAL REGISTRATION N°	
TITLE OF THE INVENTION	
	METHOD FOR MATCHING A NUMBER N OF RECEPTION TERMINALS WITH A NUMBER M OF CONDITIONAL ACCESS CONTROL CARDS
THE APPLICANT(S) OR AGENT(S)	
DESIGNATE AS INVENTOR(S):	
Inventor 1	
Name	BEUN
Forenames	Frédéric
Street	30, avenue Guy de Maupassant
Postcode and town/city	78400 CHATOU - FRANCE
Company to which attached	
Inventor 2	
Name	BOUDIER
Forenames	Laurence
Street	30, avenue Guy de Maupassant
Postal code and town	78400 CHATOU - FRANCE
Company to which attached	

Law n° 78-17 of 6 January 1978 on computerised data, files and personal rights applies to the answers given in this form. It guarantees the applicant's right to access and correct the information held by the INPI office.

Signed by
Signatory: FR, BREVALEX, G. Poulin
Certificate issuer: DE, D-Trust GmbH, D-Trust for EPO 2.0
Position
Authorised agent (Agent 1)

METHOD FOR MATCHING A NUMBER N OF RECEPTION TERMINALS WITH A NUMBER M OF CONDITIONAL ACCESS CONTROL CARDS

Technical field

The invention is in the field of security of broadcast digital data and reception equipment intended to receive these data in a data and/or services distribution network and is more specifically related to a method for matching a number N of items of data reception equipment with a number M of external security modules, each item of reception equipment being provided with a unique identifier, and each external security module having a unique identifier.

The invention also relates to reception equipment that can be matched with a plurality of external security modules to manage access to digital data distributed by an operator.

State of the prior art

More and more operators are offering data and on-line services accessible from terminals provided with security processors. In general, distributed data and services are scrambled when being sent by using secret keys, and are descrambled on reception using the same secret keys previously provided to the subscriber.

Apart from conventional access control techniques based on scrambling when sending and descrambling on reception of the distributed data, operators offer techniques based on matching of the reception terminal with a security processor to prevent the distributed data and services from being accessible to users who are using a stolen terminal or a pirated card.

Document WO 99 57901 describes a matching mechanism between a receiver and a security module based firstly on encryption and decryption of information exchanged between the receiver and the security module by a unique key stored in the receiver or in the security module, and secondly on the presence of a receiver number in the security module.

One disadvantage of this technique is due to the fact that the association between a receiver and the security module matched thereto is set up in advance, and the operator cannot efficiently manage the installed base of reception equipment to prevent this equipment being used improperly for fraudulent purposes.

One aim of the matching method according to the invention is that of enabling each operator to limit use of the installed base of reception equipment by dynamically controlling configuration of the reception equipment and external security modules intended to cooperate with this equipment.

Presentation of the invention

The invention recommends a method for matching a number N items of data reception equipment with a number M of external security modules, each item of reception equipment being provided with a unique identifier, and each external security module having a unique identifier, this method comprising a configuration phase and a check phase.

According to the invention, the configuration phase comprises the following steps:

- memorising a list of identifiers of reception equipment in each external security module,

- memorising a list of identifiers of external security module in each item of reception equipment,

and the check phase consists of authorising access to data if the identifier of an external security module connected to an item of reception equipment is present in the list memorised in this reception equipment, and if the identifier of said reception equipment is present in the list memorised in said external security module, otherwise disrupting access to said data.

Preferably, the configuration is used only when the user connects an external security module to an item of reception equipment.

In one preferred embodiment, the method according to the invention comprises a step in which the operator transmits a signal to the reception equipment to manage the check phase comprising at least one of the following set values:

- activating the check phase on a programmed date or after a programmed delay,

- deactivating the check phase on a programmed date or after a programmed delay,

- specifying an absolute date (or a delay) from which (or after which) the check phase is activated or deactivated,

- cancelling said programmed date (or said programmed delay).

In a first alternative embodiment, the operator also transmits a signal to the reception equipment

containing a message to delete the list of identifiers memorised in the reception equipment.

Said signal message is transmitted to said reception equipment through an EMM (Entitlement Management Message) specific to this item of reception equipment.

This signal may be transmitted to a group of reception equipment through an EMM message specific to said group of reception equipment.

In a second alternative embodiment, the operator also transmits a signal to the external security module containing a message to delete the list of identifiers memorised in this external security module. Said signal message is transmitted to said external security module through a specific EMM message, and can be transmitted to a group of external security modules through an EMM message specific to said group of external security modules.

According to a further feature of the method according to the invention, the operator transmits firstly the list of M identifiers of external security modules to an item of reception equipment through an EMM message specific to said reception equipment, and secondly the list of N identifiers of reception equipment to an external security module through an EMM message specific to said external security module.

According to a further alternative embodiment, the operator transmits firstly the list of M identifiers of external security modules to a group of reception equipment through an EMM message specific to the group of reception equipment, and secondly the list of N

identifiers of reception equipment to a group of external security modules through an EMM message specific to said group of external security modules.

In a further alternative embodiment, the operator transmits a signal message for the check phase to a group of reception equipment in a private flow that is processed by a dedicated software executable in each item of reception equipment as a function of the identifier of said reception equipment.

Alternatively, the list of identifiers of external security modules is transmitted in a private flow to a group of reception equipment and is processed by dedicated software executable in each item of reception equipment as a function of the identifier of said reception equipment, and the list of identifiers of reception equipment is transmitted to a group of external security modules in a private flow that is processed by dedicated software executable in each of said external security modules or in the reception equipment to which one of said external security modules is connected, as a function of the identifier of said external security module.

In one example of application of the method according to the invention, the digital data represent audiovisual programmes distributed in clear or in scrambled form.

According to a further feature, the list of identifiers of the M security modules memorised in an item of reception equipment is encrypted, and the list of identifiers of the N items of reception equipment memorised in an external security module is encrypted.

Advantageously, the method according to the invention also includes a mechanism designed to prevent use of an EMM transmitted to the same external security module or to the same reception equipment.

EMM messages specific to a security module or a reception equipment are in the following format:

```
EMM-U_section() {
table_id = 0x88                 8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-U_section_length            12 bits
unique_address_field            40 bits
for (i=0; i<N; i++) {
    EMM_data_byte               8 bits
    }
}
```

EMM messages specific to all external security modules or to all reception equipment are in the following format:

```
EMM-G_section() {
table_id = 0x8A or 0x8B         8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-G_section_length            12 bits
for (i=0; i<N; i++) {
    EMM_data_byte               8 bits
    }
}
```

EMMs specific to a sub-group of external security modules or a sub-group of reception equipment are in the following format:

```
EMM-S_section() {
table_id = 0x8E                    8 bits
section_syntax_indicator = 0       1 bit
DVB_reserved                       1 bit
ISO_reserved                       2 bits
EMM-S_section_length               12 bits
shared_address_field               24 bits
reserved                           6 bits
data_format                        1 bit
ADF_scrambling_flag                1 bit
for (i=0; i<N; i++) {
    EMM_data_byte                  8 bits
    }
}
```

The method according to the invention is used in an access control system containing a plurality of items of reception equipment each with a unique identifier and capable of cooperating with a plurality of external security modules each with a unique identifier, each external security module containing information about a subscriber's access rights to digital data distributed by an operator, this system also including a commercial management platform communicating with said reception equipment and with said external security modules. This system also includes:

- a first module arranged in said commercial management platform and designed to generate matching queries,

- and a second module arranged in said reception equipment and external security modules and designed to process said queries to prepare a matching configuration.

The method according to the invention can be used in an architecture in which the reception equipment includes a decoder and the external security module comprises an access control card in which information about a subscriber's access rights to digital data distributed by an operator are memorised. In this case, matching is performed between said decoder and said card.

Alternatively, the method according to the invention can be used in an architecture in which the reception equipment includes a decoder and the external security module includes a removable security interface provided with non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards to manage access to digital data distributed by an operator. In this case, matching is performed between said decoder and said removable security interface.

The method according to the invention can also be used in an architecture in which the reception equipment includes a decoder provided with a removable security interface with non-volatile memory designed to cooperate firstly with said decoder and secondly with a plurality of conditional access control cards. In this

case, matching is performed between said removable security interface and said access control cards.

The invention also relates to reception equipment that can be matched with a plurality of external security modules to manage access to digital data distributed by an operator. This reception equipment includes:

- non-volatile memory intended to memorise a list of external security modules.

- means for verifying whether the identifier of an external security module connected to said equipment is present in the list memorised in said non-volatile memory.

In a first embodiment, this reception equipment includes a decoder and the external security module is an access control card containing information about the access rights of a subscriber to said digital data, matching being performed in this case between said decoder and said card.

In a second embodiment, this reception equipment includes a decoder and the external security module is a removable security interface provided with non-volatile memory that will cooperate firstly with said decoder and secondly with a plurality of conditional access control cards to manage access to said digital data, matching being performed in this case between said decoder and said removable security interface.

In a third embodiment, this reception equipment includes a decoder provided with a removable security interface with non-volatile memory and intended to cooperate firstly with said decoder and secondly with a

plurality of conditional access control cards and matching is performed between said removable security interface and said access control cards.

The invention also relates to a decoder that can cooperate with a plurality of external security modules to manage access to audiovisual programmes distributed by an operator, each external security module having a unique identifier and comprising at least one data processing algorithm. This decoder comprises:

- non-volatile memory intended to memorise a list of external security modules,

- means for verifying whether the identifier of an external security module connected to said decoder is present in the list memorised in said non-volatile memory.

In a first alternative embodiment, said external security modules are access control cards in which information about access rights of a subscriber to digital data distributed by an operator are memorised.

In a second alternative embodiment, said external security modules are removable security interfaces comprising non-volatile memory and designed to cooperate firstly with the decoder and secondly with a plurality of conditional access control cards to manage access to digital data distributed by an operator.

The invention also relates to a removable security interface designed to cooperate firstly with an item of reception equipment and secondly with a plurality of conditional access control cards, to manage access to digital data distributed by an operator, each card having a unique identifier and containing information

about access rights of a subscriber to said digital data.

This interface comprises:

- non-volatile memory intended to memorise a list of subscriber cards,

- means for verifying whether the identifier of a card associated with said interface is present in the list memorised in said non-volatile memory.

In a first example embodiment, the removable interface is a PCMCIA (Personal Computer Memory Card International Association) card including digital data descrambling software.

In a second example embodiment, the removable interface is software that can be executed either in the reception equipment or in an access control card.

The method is controlled by a computer program executable on N items of reception equipment that can be matched with M external security modules each with a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, this program comprises instructions for memorising a list of identifiers of part or all of N items of reception equipment in each external security module, and instructions to memorise a list of identifiers of part or all of the M external security modules in each item of reception equipment, instructions to control the identifier of an external security module connected to an item of reception equipment and the identifier of said reception equipment, and instructions to prevent access to said data if the identifier of the external security module

connected to the reception equipment is not present in the list of identifiers previously memorised in this item of reception equipment or if the identifier of said reception equipment is not present in the list of identifiers previously memorised in said external security module.

Brief description of the drawings

Further features and advantages of the invention will become clear from the following description given as a non-limitative example with reference to the appended figures in which:

- figure 1 shows a first system architecture for use of matching according to the invention,

- figure 2 shows a second system architecture for use of matching according to the invention,

- figure 3 shows a third system architecture for use of matching according to the invention,

- figure 4 shows the structure of EMM_decoder messages for configuration and use of matching functions according to the invention,

- figure 5 shows the structure of EMM_card messages for configuration of matching functions according to the invention,

- figure 6 is a functional diagram schematically showing the states of the matching function onboard an item of reception equipment,

- figure 7 shows a flowchart illustrating a particular embodiment of matching according to the invention.

Detailed description of particular embodiments

The invention will now be described within the framework of an application in which an operator broadcasting audiovisual programmes uses the method according to the invention to limit use of his reception equipment to its own subscribers.

The method may be used in three distinct architectures shown in figures 1, 2 and 3 respectively. Identical elements in these three architectures are denoted by identical references.

Matching is managed from a commercial platform 1 controlled by the operator and communicating with reception equipment installed at the subscriber end.

In the first architecture shown in figure 1, the reception equipment includes a decoder 2 in which access control software 4 is installed, and the external security module is an access control card 6 containing information about access rights of a subscriber to broadcast audiovisual programmes. In this case, matching is performed between the decoder 2 and the card 6.

In the second architecture shown in figure 2, the reception equipment includes a decoder 2 not dedicated to access control, and the external security module is a removable security interface 8 provided with non-volatile memory and in which the access control software 4 is installed. This interface 8 cooperates firstly with said decoder 2, and secondly with a card 6 among a plurality of conditional access control cards, to manage access to said audiovisual programmes.

In this architecture, matching is performed between said removal security interface 8 and said access control card 6.

In the third architecture shown in figure 3, the reception equipment includes a decoder 2 in which an access control software 4 is installed, and which is connected to a removable security interface 8 with non-volatile memory designed to cooperate firstly with said decoder 2, and secondly with a card 6 from a plurality of conditional access control cards.

In this case, matching is performed between the decoder 2 and the removable security interface 8.

The configuration and use of matching by the operator is the result of commands sent by the commercial management platform 1 installed at the operator end.

The following description relates to use of the invention in the case of matching of N dedicated decoders 2 with M cards 6. The steps used are applicable to the three architectures described above.

All matching processing is inactive when N decoders 2 leave the factory, and also after access control software 4 has been downloaded onto each decoder 2. In particular:

- no card identifier is memorised in the decoders 2,
- checking of card identifiers 6 by the decoders 2 is not active,
- checking by decoders 2 that the presence of the identifier thereof in cards 6 is not active.

Similarly, when the M cards 6 leave the factory, there is no identifier decoder 2 memorised in the cards 6.

Matching can then be configured and used in the N decoders 2 and in the M cards 6 by a query from the operator through the management platform 1 that sends:

- EMM_decoder messages dedicated to matching, to the N decoders 2.

- EMM_card messages dedicated to matching, to the M cards 6. These EMM_card messages are sent to the cards 6 directly or are integrated into EMM_decoder messages.

EMM_decoder messages perform the following tasks:

- activate the matching function in the N decoders 2. In this case, each decoder verifies whether the identifier of a card 6 inserted in the decoder card reader forms part of the identifiers memorised and that the identifier of this decoder 2 forms part of the identifiers of decoders memorised in this card 6. If this is not the case, a disruption is applied in the access to data.

- deactivate the matching function in the N decoders 2. In this case, each decoder 2 does not check the identifier thereof or the identifier of the card.

- load the list of M identifiers of cards 6 matched to the N decoders 2, into these decoders.

- erase identifiers of cards 6 already memorised in the N decoders 2.

EMM_card messages:

- load the list of N identifiers of decoders 2 matched to these cards, in the M cards 6.

- erase the identifiers of decoders 2 already memorised in the M cards 6.

Addressing of EMM messages

EMM messages used for configuration and use of functions related to matching according to the method according to the invention are sent in an EMM channel of a digital multiplex as defined by the MPEG2/System standard and DVB/ETSI standards.

This channel can broadcast EMMs referencing a card address so that they can be addressed directly to:

- a particular card,
- cards in a particular group,
- all cards,

This channel can also broadcast EMMs referencing a decoder address so that they can be addressed directly to:

- a particular decoder,
- a particular group of decoders,
- all decoders,

Messages intended for a particular card or for a particular decoder are EMM-U messages with the following structure:

```
EMM-U_section() {
table_id = 0x88                  8 bits
section_syntax_indicator = 0     1 bit
DVB_reserved                     1 bit
ISO_reserved                     2 bits
EMM-U_section_length             12 bits
unique_address_field             40 bits
for (i=0; i<N; i++) {
```

```
        EMM_data_byte                8 bits
        }
    }
```

The unique_address_field parameter is the unique address of a card in a card EMM-U or the unique address of a decoder in a decoder EMM-U.

Messages intended for cards in a particular group of cards or decoders in a particular group of decoders are EMM-S messages with the following structure:

```
    EMM-S_section() {
    table_id = 0x8E                8 bits
    section_syntax_indicator = 0   1 bit
    DVB_reserved                   1 bit
    ISO_reserved                   2 bits
    EMM-S_section_length           12 bits
    shared_address_field           24 bits
    reserved                       6 bits
    data_format                    1 bit
    ADF_scrambling_flag            1 bit
    for (i=0; i<N; i++) {
        EMM_data_byte              8 bits
        }
    }
```

The shared_address_field parameter is the address of the group of cards in a card EMM-S or the address of the group of decoders in a decoder EMM-S. A decoder in a group or a card in a group is concerned by the message if it is also explicitly designated in an ADF field contained in EMM_data_byte and that can be encrypted using the ADF_scrambling_flag information.

Messages intended for all cards or all decoders are EMM-G messages with the following structure:

```
EMM-G_section() {
table_id = 0x8A or 0x8B          8 bits
section_syntax_indicator = 0     1 bit
DVB_reserved                     1 bit
ISO_reserved                     2 bits
EMM-G_section_length             12 bits
for (i=0; i<N; i++) {
    EMM_data_byte                8 bits
    }
}
```

Content of decoder EMM messages

Figure 4 schematically shows the content of EMM_data_byte data in a matching EMM_decoder message. This content depends on the function to be executed by a decoder 2 for configuration or use of matching.

EMM_data_byte data include the following functional parameters:

- ADF 20: address complement of a decoder in a group of decoders; this parameter is useful for addressing by group, otherwise it can be omitted; it can be encrypted.

- SOID 22: identification of matching message according to the invention, from other types of messages.

- OPID/NID 24: identification of the group of decoders and the operator's signal.

- TIME 26: time dating data for sending the message; this parameter is used to avoid the need to replay the message by the same decoder

- CRYPTO 28: identification of cryptographic protection functions applied to FUNCTIONS parameters 32; FUNCTIONS parameters can be encrypted and protected by a cryptographic redundancy 30.

- FUNCTIONS 32: set of parameters describing the configuration and use of matching.

- STBID 34: unique address of the decoder concerned by the message. This parameter is present in a decoder EMM-U, otherwise it can be omitted.

The above functional parameters are freely organised in the EMM_data_byte data of an EMM_decoder message. One preferred implementation is the combination of these parameters by a T L V (Type Length Value) structure.

Content of EMM_card messages

Figure 5 schematically shows the content of EMM_data_byte data in a matching EMM_Card message. This content is used to write, modify or erase a list of terminal identifiers.

EMM_data_byte data include the following functional parameters:

- SOID 40: operator identification.

- ADF 42: addressing complement of a card in a group of cards; this parameter is useful when addressing by group, otherwise it can be omitted; it can be encrypted.

- CRYPTO 44: identification of cryptographic protection functions applied to the LDA parameter 48 and to other parameters 50; parameters 48 and 50 can be encrypted and protected by cryptographic redundancy 46.

- LDA 48 (List of authorised decoders): this parameter contains the list of decoder identifiers with which the card can operate.

EMM_data_byte data can also contain other parameters 50 concerning functions of the card other than matching.

Parameters in the EMM_data_byte data are freely organised in these data of a card EMM message. One preferred implementation is the combination of these parameters by a T L V (Type Length Value) structure.

Configuration and use of matching

The set of FUNCTIONS parameters 32 in an EMM_decoder describes the configuration and use of matching according to the invention. This set of parameters is any combination of the following functional parameters:

- MODE: this parameter activates, deactivates or resets the matching solution according to the invention. After deactivation, the decoder does not check the identifier of a card inserted, but keeps the list of memorised identifiers. After resetting, the decoder does not check the identifier of an inserted card and no longer has any memorised card identifiers

- LCA (List of authorised cards): this parameter loads the list of card identifiers with which it can operate, in a decoder

- Disruption: this parameter describes the disruption to be applied by the decoder in the data access in the case of a card not matched with the decoder

- Date/Delay: this parameter characterises the matching activation or deactivation date or delay.

The above functional parameters are freely organised in all FUNCTIONS parameters 32. One preferred implementation is the combination of these parameters by a T L V (Type Length Value) structure.

Furthermore, in some types of service such as a form of matching a decoder with a card, an EMM_decoder can transport one or a plurality of EMM_cards. In this case, the EMM_card(s) is (are) included in the set of FUNCTIONS parameters 32 in a manner that can be clearly identified by the decoder that can extract and provide the EMM_card(s) to the inserted card. One preferred implementation of including EMM_card in the set of FUNCTIONS parameters 32 of an EMM_decoder is that of using a particular T L V structure containing EMM_card(s) with all related addressing data.

A further use of EMM_card in an EMM_decoder is that of memorising that this EMM_decoder has already been processed by the decoder, in the card, so as to avoid a replay on another decoder so that this EMM can be processed once only by a single decoder; semantically, these data mean "Already processed" and are verified by the access control software 4 of the decoder 2 when processing this EMM. One preferred embodiment of this anti-replay mechanism is that

writing these data in a FAC (Facilities Data Block) data block on the card.

Operation

Operation of matching according to the invention will now be described with reference to figures 6 and 7.

Figure 6 is a functional diagram schematically showing states of the matching function of the access control software 4 onboard a decoder 2.

The matching function is in the inactive state 60 when the access control software 4 has just been installed or downloaded 61, or when it has received a deactivate matching order 62 or reset matching order 64 from the management platform 1. In this state, the access control software 4 will operate with a card 6 inserted in the decoder 2 without verifying matching with this card.

In order to activate matching between M decoders 2 and N cards 6, the operator activates the following through the management platform 1:

- processing 70 to define the matching mode (= active), and the applicable disruption type in access to data if matching fails,

- processing 72 to define the LCA list to be loaded in these N decoders of identifiers of M authorised cards,

- processing 74 to define the LDA list to be loaded in these M cards of identifiers of N authorised decoders

Based on this information, the management platform 1 generates and sends (arrow 76):

-- at least one EMM_decoder message to load the LCA list of authorised cards 6 into the non-volatile memory of the N decoders 2.

-- at least one EMM_card message to load the LDA list of authorised decoders into the non-volatile memory of M cards 6

-- at least one EMM_decoder message to load configuration parameters into the non-volatile memory of the N decoders 2.

The matching function in a decoder 2 changes to the active state 78.

During activation of the matching function in a decoder 2 with loading of the LCA list of authorised cards 6 and/or the LDA list of authorised decoders 2, the configuration parameters may be taken into account by a decoder 2 with a time delay defined by the Date/Delay parameter to guarantee effective loading of the LCA list of authorised cards 6 into a decoder 2 and the LDA list of authorised decoders 2 in a card 6.

During reactivation of the matching function in a decoder 2, if the LCA list of authorised cards 6 and/or the LDA list of authorised decoders 2 does not have to be changed, the corresponding EMMs are neither generated nor sent.

The operator may deactivate (step 80) matching in a decoder 2, from the management platform 1 that generates and sends (arrow 82) an EMM message addressing the decoder(s) 2 concerned and containing a deactivation order without erasing the matching context 62 or a RESET order of the matching context 64.

The matching function in a decoder 2 changes to the inactive state 60.

Effective acceptance of the deactivation order by a decoder 2 may be delayed in time as defined by the Date/Delay parameter.

Regardless of the state of a matching function, whether inactive 60 or active 78, it may receive a list of authorised LCA cards 6 through the decoder EMM (step 72) or a list of authorised LDA decoders 2 (step 74) from the management platform 1.

Acceptance of one of the M cards 6 by the matching function of one of N decoders 2 is described in the flowchart in figure 7.

When a card 6 is inserted (step 100) into the decoder 2, the onboard access control software 4 in the decoder tests (step 102) whether the matching function is in the active state 78.

If the matching function in the decoder is in the inactive state 60, the decoder will operate with the inserted card (108).

If the matching function in the decoder is in the active state 78, the access control software:

- reads the identifier of the inserted card and verifies (step 104) whether this identifier is in the list of authorised cards 6 memorised in the decoder 2,
- reads the list of authorised decoders in the inserted card and verifies (step 106) whether the identifier of the decoder 2 is present in this list,

The tests 104 and 106 may be executed in any order.

If the results of these two identifier tests 104 and 106 are positive, the access control software 4

accepts to operate with the inserted card 6 (step 108). Broadcast programmes can then be accessed, provided that other access conditions attached to these programmes are conforming.

If the result of at least one of the tests 104 and 106 is not positive, the access control software 4 refuses to operate with the inserted card 6 and applies (step 110) the disruption in data access as defined by the operator. Such a disruption may consist of blocking access to broadcast programmes. It may be accompanied by a message prompting the subscriber to insert another card 6 in the decoder 2, being displayed on the screen of the terminal with which the decoder is associated.

When the card 2 is removed (step 112) from the decoder 2, the access control software starts waiting for a card to be inserted (step 100)

The disruption applied in step 110 in access to data in the case of a matching fault may be of different natures, such as:

- Stop audio and video on encrypted channels (obtained by not submitting ECMs to the card to calculate CWs);

- Stop audio and video on clear format and analogue channels (obtained by a message to the middleware);

- Send a message to the terminal middleware (example: Open TV message).

This disruption may also be used to block stolen decoders.

In the case described in figure 2 in which the access control software 4 is executed in the removable

interface 8 connected to a decoder 2, the logic controller described in figure 4 and the flowchart described in figure 5 are applicable directly to the onboard access control software 4 in this removable interface 8.

CLAIMS

1. Method for matching a number N of items of data reception equipment (2) with a number M of external security modules (6, 8), each item of reception equipment (2) being provided with a unique identifier, and each external security module (6, 8) having a unique identifier, method characterised in that it comprises a configuration phase comprising the following steps:

- memorising a list of identifiers of reception equipment (2) in each external security module (6, 8),

- memorising a list of identifiers of external security module (6, 8) in each item of reception equipment (2),

and a check phase consisting of authorising access to data if the identifier of an external security module (6, 8) connected to an item of reception equipment (2) is present in the list memorised in this reception equipment (2), and if the identifier of said reception equipment (2) is present in the list memorised in said external security module (6, 8), otherwise disrupting access to said data.

2. Method according to claim 1, characterised in that the configuration is used only when the user connects an external security module (6, 8) to an item of reception equipment (2).

3. Method according to claim 1, characterised in that the method also comprises a step in which the

operator transmits a signal to the reception equipment (2) to manage the check phase comprising at least one of the following set values:

- activating the check phase on a programmed date or after a programmed delay,
- deactivating the check phase on a programmed date or after a programmed delay,
- specifying an absolute date (or a delay) starting from which (or after which) the check phase is activated or deactivated,
- cancelling said programmed date (or said programmed delay).

4. Method according to claim 1, characterised in that the operator also transmits a signal to the reception equipment (2) containing a message to delete the list of identifiers memorised in the reception equipment (2).

5. Method according to claim 1, characterised in that the operator also transmits a signal to the external security module (6, 8) containing a message to delete the list of identifiers memorised in this external security module (6, 8).

6. Method according to claim 1, characterised in that the operator transmits the list of M identifiers of the external security modules (6, 8) to an item of reception equipment (2) through an EMM message specific to said reception equipment (2).

7. Method according to claim 1, characterised in that the operator transmits the list of identifiers of N items of reception equipment (2) to an external security module (6, 8) through an EMM message specific to said external security module (6, 8).

8. Method according to claim 1, characterised in that the operator transmits the list of M identifiers of external security modules (6, 8) to a group of reception equipment (2) through an EMM message specific to said group of reception equipment (2).

9. Method according to claim 1, characterised in that the operator transmits the list of identifiers of N items of reception equipment (2) to a group of external security modules (6, 8) through an EMM message specific to said group of external security modules (6, 8).

10. Method according to claims 3 or 4, characterised in that the operator supplies said signal message to an item of reception equipment (2) through an EMM message specific to said reception equipment (2).

11. Method according to claims 3 or 4, characterised in that the operator supplies said signal message to a group of reception equipment (2) through an EMM message specific to said group of reception equipment (2).

12. Method according to claim 5, characterised in that the operator supplies said signal message to an external security module through an EMM message specific to said external security module (2).

13. Method according to claim 5, characterised in that the operator supplies said signal message to a group of external security modules (6, 8) through an EMM message specific to said group of external security modules (6, 8).

14. Method according to claims 3 or 4, characterised in that the operator transmits a signal message to a group of reception equipment (2) in a private flow for the check phase, said private flow being processed by dedicated software executable in each item of reception equipment (2) as a function of the identifier of said reception equipment (2).

15. Method according to claim 1, characterised in that the list of identifiers of external security module (6, 8) is transmitted in a private flow to a group of reception equipment (2) and processed by dedicated software executable in each item of reception equipment (2) as a function of the identifier of said reception equipment (2).

16. Method according to claim 1, characterised in that the list of identifiers of reception equipment (2) is transmitted to a group of external security modules (6, 8) in a private flow that is processed by

dedicated software in each of said external security modules (6, 8) or in the reception equipment (2) to which each of said external security modules (6, 8) is connected, as a function of the identifier of said external security module (6, 8).

17. Method according to claim 1, characterised in that digital data are distributed in clear or in scrambled form.

18. Method according to claim 17, characterised in that digital data are audiovisual programmes.

19. Method according to claim 1, characterised in that the list of identifiers of M security modules memorised in an item of reception equipment (2) is encrypted.

20. Method according to claim 1, characterised in that the list of identifiers of N items of reception equipment (2) memorised in an external security module (6, 8) is encrypted.

21. Method according to any of claims 6 to 13, characterised in that the method also includes a mechanism designed to prevent use of an EMM transmitted to the same external security module (6, 8) or to the same item of reception equipment (2).

22. Method according to claims 6, 7, 10 or 12, characterised in that said EMM is in the following format:

```
EMM-U_section() {
    table_id = 0x88                 8 bits
    section_syntax_indicator = 0    1 bit
    DVB_reserved                    1 bit
    ISO_reserved                    2 bits
    EMM-U_section_length            12 bits
    unique_address_field            40 bits
    for (i=0; i<N; i++) {
        EMM_data_byte               8 bits
        }
    }
```

23. Method according to claims 8, 9, 11 or 13, characterised in that said EMM message concerns all external security modules (6, 8) or all items of reception equipment (2) and is in the following format:

```
EMM-G_section() {
    table_id = 0x8A or 0x8B         8 bits
    section_syntax_indicator = 0    1 bit
    DVB_reserved                    1 bit
    ISO_reserved                    2 bits
    EMM-G_section_length            12 bits
    for (i=0; i<N; i++) {
        EMM_data_byte               8 bits
        }
    }
```

24. Method according to claims 8, 9, 11 or 13, characterised in that said EMM message is specific to a sub-group of external security modules (6, 8) or a sub-group of reception equipment (2) and is in the following format:

```
EMM-S_section() {
table_id = 0x8E                 8 bits
section_syntax_indicator = 0    1 bit
DVB_reserved                    1 bit
ISO_reserved                    2 bits
EMM-S_section_length            12 bits
shared_address_field            24 bits
reserved                        6 bits
data_format                     1 bit
ADF_scrambling_flag             1 bit
for (i=0; i<N; i++) {
    EMM_data_byte               8 bits
    }
}
```

25. Method according to any of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder and the external security module (6, 8) includes an access control card (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised, and in that matching is performed between said decoder and said card (6).

26. Method according to any of claims 1 to 24, characterised in that the reception equipment (2)

includes a decoder and the external security module (6, 8) includes a removable security interface (8) provided with non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator, and in that matching is performed between said decoder and said removable security interface (8).

27. Method according to any of claims 1 to 24, characterised in that the reception equipment (2) includes a decoder provided with a removable security interface (8) with non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6) and in that matching is performed between said removable security interface (8) and said access control cards (6).

28. Reception equipment that can be matched with a plurality of external security modules (6, 8) to manage access to digital data distributed by an operator, characterised in that it includes:

- non-volatile memory intended to memorise a list of external security modules (6, 8),

- means for verifying whether the identifier of an external security module (6, 8) connected to said equipment is present in the list memorised in said non-volatile memory.

29. Equipment according to claim 28, characterised in that the equipment includes a decoder and in that the external security module (6, 8) is an access control card (6) containing information about access rights of a subscriber to said digital data, matching being performed between said decoder and said card (6).

30. Equipment according to claim 28, characterised in that the equipment includes a decoder and in that the external security module (6, 8) is a removable security interface (8) provided with non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6), to manage access to said digital data, matching being performed between said decoder and said removable security interface (8).

31. Equipment according to claim 28, characterised in that the equipment includes a decoder provided with a removable security interface (8) with non-volatile memory and designed to cooperate firstly with said decoder, and secondly with a plurality of conditional access control cards (6) and in that matching is performed between said removable security interface (8) and said access control cards (6).

32. Decoder that can cooperate with a plurality of external security modules (6, 8) to manage access to audiovisual programmes distributed by an operator, each external security module (6, 8) having a single

identifier and comprising at least one data processing algorithm, characterised in that it includes:

- non-volatile memory designed to memorise a list of external security modules (6, 8),

- means for verifying whether the identifier of an external security module (6, 8) connected to said decoder is present in the list memorised in said non-volatile memory.

33. Decoder according to claim 32, characterised in that said external security modules (6, 8) are access control cards (6) in which information about access rights of a subscriber to digital data distributed by an operator is memorised.

34. Decoder according to claim 32, characterised in that said external security modules (6, 8) are removable security interfaces (8) including non-volatile memory and designed to cooperate firstly with the decoder, and secondly with a plurality of conditional access control cards (6) to manage access to digital data distributed by an operator.

35. Removable security interface designed to cooperate firstly with an item of reception equipment (2), and secondly with a plurality of conditional access control cards (6), to manage access to digital data distributed by an operator, each card having a unique identifier and containing information about access rights of a subscriber to said digital data, characterised in that it includes:

- non-volatile memory designed to memorise a list of subscriber cards,

- means for verifying whether the identifier of a card associated with said interface is present in the list memorised in said non-volatile memory.

36. Interface according to claim 35 characterised in that it consists of a PCMCIA card containing digital data descrambling software.

37. Interface according to claim 35 characterised in that it consists of software.

38. Access control system including a plurality of items of reception equipment (2) each having a unique identifier and that can cooperate with a plurality of external security modules (6, 8) each having a unique identifier, each external security module (6, 8) containing information about access rights of a subscriber to digital data distributed by an operator, said system also including a commercial management platform (1) communicating with said reception equipment (2) and said external security modules (6, 8), characterised in that is also includes:

- a first module arranged in said commercial platform (1) and designed to generate matching queries,

- and a second module arranged in said reception equipment (2) and in said external security modules (6, 8) and designed to process said queries to prepare a matching configuration.

39. Computer program executable on N items of reception equipment (2) that can cooperate with M security modules (6, 8) each having a unique identifier and in which information about access rights of a subscriber to digital data distributed by an operator are stored, characterised in that it comprises instructions for memorising a list of identifiers of part or all of N items of reception equipment (2) in each external security module (6, 8), and instructions to memorise a list of identifiers of part or all of the M external security modules (6, 8) in each item of reception equipment (2), instructions to control the identifier of a security module connected to an item of reception equipment (2) and the identifier of said reception equipment (2), and instructions to prevent access to said data if the identifier of the security module (6, 8) connected to the reception equipment (2) is not present in the list of identifiers previously memorised in this reception equipment (2) or if the identifier of said reception equipment (2) is not present in the list of identifiers previously memorised in said external security module (6, 8).

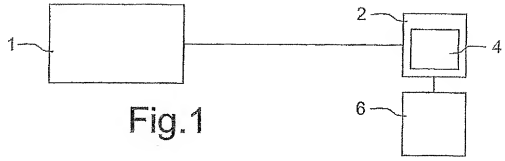

Fig.1

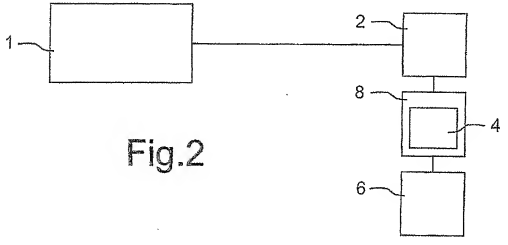

Fig.2

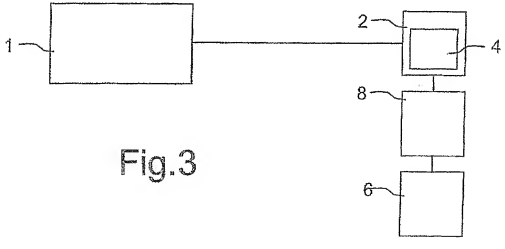

Fig.3

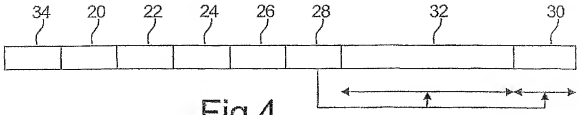

Fig.4

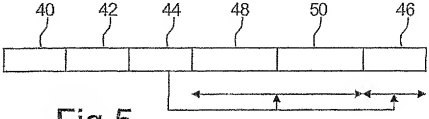

Fig.5

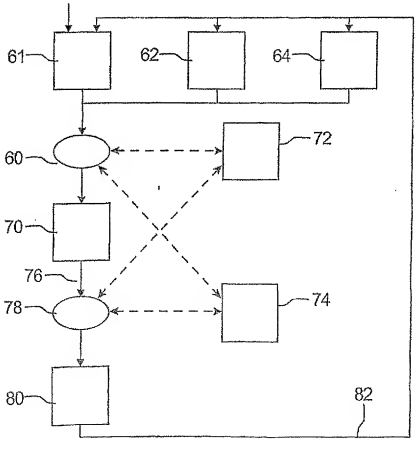

Fig.6

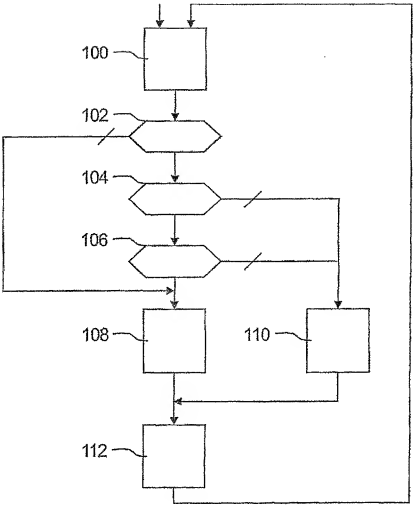

Fig.7